Cross-Layer Mischief in Networked Control Systems

Gregory Nazario, Michael Rosen, Lawrence Jackson, Michael Hankowsky
Carnegie Mellon University
Electrical & Computer Engineering
Pittsburgh, USA
{gnazario, mrrosen, lmjackso, mhankows}@andrew.cmu.edu

***Abstract*—SCADA (supervisory control and data acquisition) systems are becoming increasingly prevalent, especially wirelessly networked control systems. [citation] The integration of wireless networking into the operation of these SCADA systems is good for many reasons, but these integrations often ignore security as a priority. [citation] Our goal is to better understand the capabilities and the vulnerabilities these systems characteristically possess. In order to do this we will explore the use of cross-layer attacks on networked control systems and develop a framework for testing these attacks. We have developed testbed consists of a simulated network, a simulated factory driven by a matlab-ran Tennessee-Eastman process and the interface between these systems. Our research has confirmed that these vulnerabilities are exploitable and we have established this in our testbed. These vulnerabilities point to the necessity for a change in the way we look at securing SCADA integrated wireless networks.**

I. Introduction

The growing prevalence of SCADA systems have brought much needed attention to the class of cyberphysical threats. This paper examines the specific effects and testing of cyberphysical threats in wireless networking. Our intent is to simulate a networked control system similar to that of what one might find in a chemical plant. We approached Stuxnet destroyed a fifth of Iran's nuclear centrifuges. This is one simple example of SCADA SCADA Systems ... [more on scada]

A. The Framework

Subsection text here.

1) Subsubsection Heading Here: Subsubsection text here. at

II. Related Work

III. Approach

Our goals were to create a modular framework that:

1) allows for extension by other developers, but without specific domain knowledge
2) provides for consistent parameterized simulation
3) allows for diverse simulations tailored to realistic SCADA conditions

A. Simulated Network

B. Controller

1) Actuator:

2) Sensor:

3) Internet Cloud:

4) Factory Access Point:

5) Factory Bridge:

C. Matlab Simulation

1) Tennessee Eastman:

D. C++ to Matlab Bridge

IV. Implementation

A. Simulated Network

1) Controller:

2) Actuator:

3) Sensor:

4) Internet Cloud:

5) Factory Access Point:

6) Factory Bridge:

B. Matlab Simulation

1) Tennessee Eastman:

C. C++ to Matlab Bridge

V. Challenges

A. Omnet++

B. Matlab

C. Bridge

VI. Evaluation

A. Metrics

We will consider three metrics when evaluating the results of our experimentation: sensor data, control signals and packet throughput.

1) Sensor Data: We consider Sensor Data because this includes crucial data about what is actually occurring in the simulated plant process (Tennessee-Eastman, in this case).

2) Control Signals: We consider the Control signals because these signals are meant to be directing the process, and how they react when parameters of the simulation are changed a crucial to our understanding of how various attacks effect our simulation.

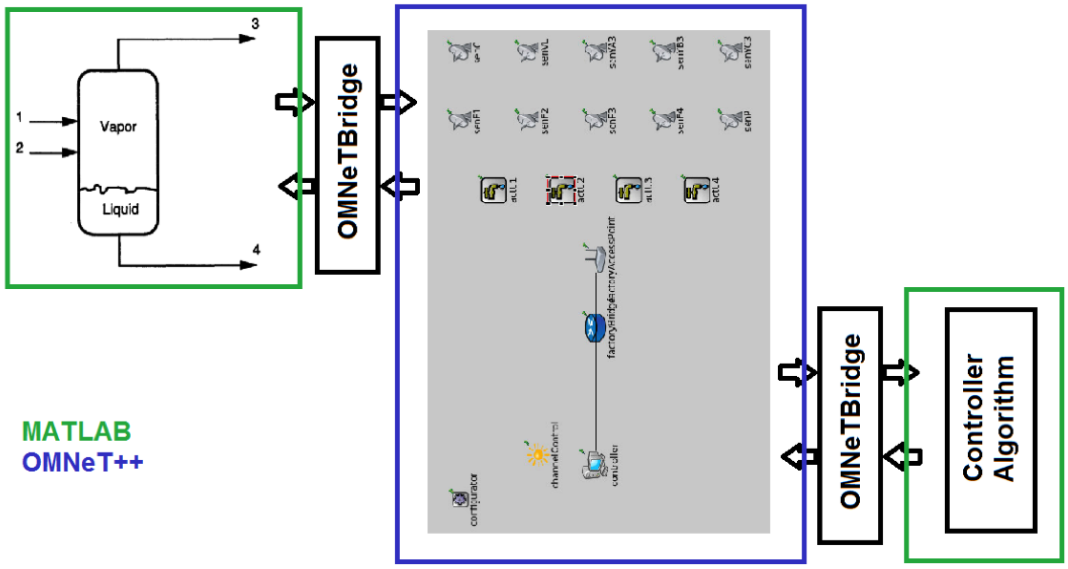

Fig. 1. System Diagram.

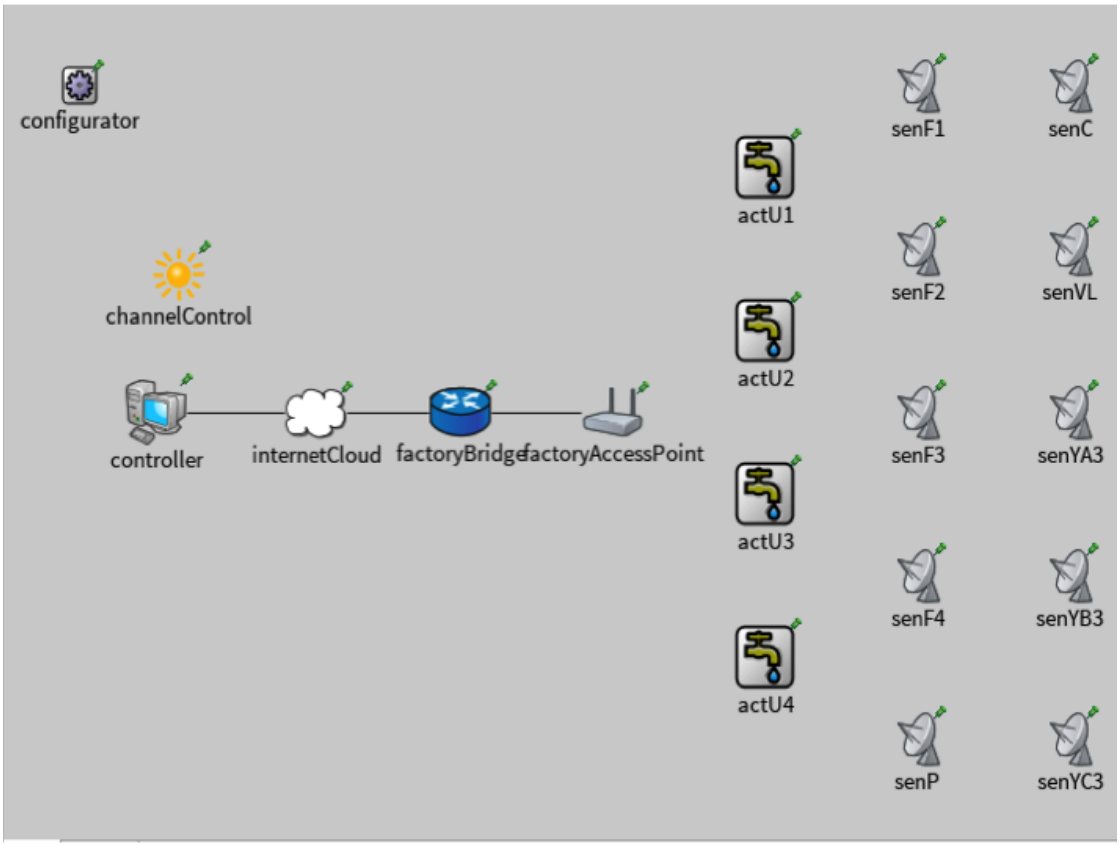

Fig. 2. Network Diagram.

3) Throughput: We use the packet throughput as an evaluation metric because this data is extremely relevant in denial of service type attack we have implemented.

VII. Attacks

A. DDoS

VIII. Discussion

IX. Future Work

A large goal of this project was to develop a framework that would enable further research to be done in this space. What we've provided makes it very easy to develop different network configurations for corresponding process simulations in Matlab. There are three major fields of further work that we propose: extending the framework, experimenting with more attacks and validating configurations.

A. Extending the Framework

The framework is functionally complete, but there are additions that could be made. More modules could be adapted to support a greater range of network simulations. The addition of primitives to support cryptography, or at the least simulated cryptography, would enhance the realism of this framework and allow for truer to life attacks.

B. Experimentation

A large body of future work could easily consist of just experimentation with different types of misbehavior and exploitation.

C. Validation and Research

It would be valuable to do further research into the common configurations of networked control systems in industry. This information would certainly help focus future experimentation and development.

X. Conclusion

We have developed a

Acknowledgment

The authors would like to thank Bruce DeBruhl for guiding our research and for helping us to refine our ideas.

References

[1] Siaterlis et al., *EPIC: A Testbed for Scientifically Rigorous Cyber-Physical Security Experimentation*, Vol 1, No.2 IEEE Transactions on Emerging Topics in Computing, 2013.

[2] Mo et al., *Cyber-Physical Security of a Smart Grid Infrastructure*, Vol. 100, No.1 Proceedings of the IEEE, 2012.

[3] Cardenas et al., *Challenges for Securing Cyber Physical Systems*, 2009.

[4] N. L. Ricker, *Model predictive control of a continuous, nonlinear, two-phase reactor*, Seattle, WA: University of Washington, 1993.

[5] A. Hayes, *Network Service Authentication Timing Attacks*, IEEE Computer and Reliability Societies, 2013.

[6] H. Beitollahi, G. Deconinck, *A Dependable architecture to mitigate distributed denial of service attacks on network-based control systems*, Vol.4, International Journal of Critical Infrastructure Protection, 2011.

[7] S. Radosavac, N Benahammar and JS Baras, *Cross-layer attacks in wireless ad hoc networks*,Princeton, New Jersey: Conference on Information Sciences and Systems, 2004.

[8] S. Amin, A. Cardenas and S.S. Sastry, *Safe and Secure Networked Control Systems under Denial-of-Service Attacks*, Berlin, Germany: Springer-Verlag, 2009.

[9] Hashimoto et al., *Safety securing approach against cyber-attacks for process control system*, Vol. 57,Nagoya, Japan: Computers and Chemical Engineering, 2013.

[10] Y. Mo and B. Sinopoli, *Secure Control Against Replay Attacks*, 47th Illinois, USA: Annual Alerton Conference, 2009.

[11] S. McLaughlin, *Securing Control Systems from the Inside: A Case for Mediating Physical Behaviors*,IEEE Security & Privacy, 2013.

[12] X. Chen, K. Makki, K. Yen and N. Pissinou, *Sensor Network Security: A Survey*, Vol. 11, No. 2IEEE Communications Surveys & Tutorials, 2009.